PRIVACY IMPACT ASSESSMENT

Consular Affairs Business Intelligence (CABI) Portal

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of System: Consular Affairs Business Intelligence Portal

(b) Bureau: Consular Affairs

(c) System Acronym: CABI Portal

(d) iMATRIX Asset ID Number: 6126

(e) Reason for Performing PIA:

☐ New System

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

This is a Major Application (MA) which previously did not contain Personally Identifiable Information (PII) but now does. See 3d for a description of PII being collected.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒ Yes

☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance

(b) What is the security assessment and authorization (A&A) status of the system?

The triennial Assessment and Authorization process is underway and CABI Portal is expected to renew its Authorization-To-Operate by Spring 2018.

(c) Describe the purpose of the system:

The purpose of the CABI Portal is to provide a centralized interface for Consular Affairs Business Intelligence (CABI) solutions including dashboards, reports, and ad-hoc reporting and analysis tools. The CABI Portal is the primary implementation tool of the Consular Affairs Enterprise Reporting program. The CABI Portal provides service to every office within CA. The CABI Portal provides the framework for these users to access consular data extracted from other sources through the CCD. CABI Portal pulls (Non-Immigrant Visa) NIV data from the CCD and also pulls information from the following systems: Immigrant Visa Overseas (IVO), Consular Electronic Application Center (CEAC), and Travel Document Issuance System (TDIS). The data is then aggregated and loaded into database structures optimized for reporting (also referred to as the CA Enterprise Data Warehouse and data marts).

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Names of Individuals
Birthdates of Individuals
Phone number(s) of Individuals
Personal and other Addresses
E-mail address(es) of Individuals
Government Issued IDs (e.g., passport numbers or national IDS of visa applicants; UserIds for DoS employees)
Social media accounts of individuals

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

For Passport related information

- 22 U.S.C. § 3927 (Chief of Mission)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended);
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure);
- 22 U.S.C. 211a-218, (Passports)
- 22 U.S.C. 2651a (Organization of Department of State);
- Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports);
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Residence Status)

For Visa related information

- 8 U.S.C. 1151-1363a03 (Title II - Immigration and Nationality Act of 1952, as amended);
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 C.F.R. Parts 40-42, and 46 (Visas)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, provide:

SORN Name and Number:
SORN publication date:

State-39 Visa Records, October 25, 2012
State-05 Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
State-26 Passport Records, March 24, 2015

☐ No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

☐ Yes

☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

☐ Yes

☒ No

The Bureau of Consular Affairs (CA) maintains the data within its systems indefinitely, until a records disposition schedule is approved by NARA in partnership with the Bureau of Administration (A). Currently, CA and A Bureau are coordinating to revise records schedules for CA systems. Until the records disposition schedules are approved by NARA, the records will be maintained indefinitely.

If yes provide:
Schedule number (e.g., (XX-587-XX-XXX)):
Length of time the information is retained in the system:
Type of information retained in the system:

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☐ Other (people who are not U.S. Citizens or LPRs)

Data is entered into original source databases/other systems (e.g. NIV, IVO,CEAC and TDIS) by applicants and Consular Officers which is contained in the CCD database then pulled into the CABI reporting schemas.

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐ Yes

☒ No (SSNs are not collected)

If yes, under what authorization?

(c) How is the information collected?

The information for the CABI portal reports is collected directly (database to database) from the CCD which houses information from consular systems, all of which reside outside the CABI Portal system boundary.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

The CCD information comes directly from foreign individuals who are applying for Visas, US Citizens applying for Passports, and information entered by Consular Officers into the source systems. CABI Portal only pulls data from these systems via the CCD and therefore relies on the source systems to maintain and supply accurate data.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Information from CCD is current and is pulled into the CABI Portal databases at least once a week.

(g) Does the system use information from commercial sources? Is the information publicly available?

No, the CABI Portal does not use commercial information or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

CABI Portal gets its data from other CA information systems. It does not collect any data directly from any individual.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

☐ Yes

☒ No

If yes, how do individuals grant consent?

If no, why are individuals not allowed to provide consent?

Within the CABI Portal, individuals do not have the opportunity to decline to provide information, etc., because the information is collected from the CCD database, and consent is provided at the initial point of collection.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The Department of State seeks to address privacy risks by minimizing PII in excess of what is required by CABI Portal to produce reports needed by management or to combine data from different systems correctly. For example, in a report, only an applicant identification number is utilized as opposed to a Social Security Number.

5. Use of information

(a) What is/are the intended use(s) for the information?

The information is used to generate reports and compile metrics related to consular operations and transactions, such as visa and passport applications and applicants, so that consular professionals can perform various types of analyses, including fraud detection, resource allocation, and determination of the cost of services.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

(c) Does the system analyze the information stored in it?

☒ Yes

☐ No

If yes:

(1) What types of methods are used to analyze the information?

The reports from CABI Portal display metrics based on a category, comparisons based on trends & averages, and bring together data from different systems to show relationships of the data.

(2) Does the analysis result in new information?

Yes.

(3) Will the new information be placed in the individual’s record?

☐Yes

☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

☒Yes

☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The main internal stakeholders are within Consular Affairs, with other Department of State bureaus such as Diplomatic Security (DS) and the Bureau of Population, Refugees, and Migration (PRM) occasionally requesting reports from our system. No one outside of the Department of State has access to the CABI Portal itself or the data within the underlying data warehouse.

(b) What information will be shared?

The PII mentioned in 2d will be shared through dashboards, reports, ad-hoc reporting tools, and analysis tools.

(c) What is the purpose for sharing the information?

Information is shared for the purpose of decision support, operational improvement, workload assessment and forecasting, resource planning, and fraud analysis and investigation reports for use by Consular Affairs.

(d) The information to be shared is transmitted or disclosed by what methods?

After the CABI Portal manipulates the data and produces an electronic report or file, the authorized user can then save it on a local or network drive, or send it as an email attachment. The report can also be printed or faxed.

(e) What safeguards are in place for each internal or external sharing arrangement?

Security Officers determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted. Safeguards include secure transmission methods permitted by State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. Internal sharing requires a connection agreement and OpenNet users with privileged role based access to manage the connection.

Regularly-administered security/privacy training is provided to all OpenNet users regarding proper handling procedures.

CABI Portal reports are currently available only to Department of State CA users.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns associated with the CABI Portal include (1) unauthorized access/disclosure or (2) modification of the data.

Unauthorized Access/Disclosure: The CABI Portal has a very restrictive policy regarding accessing sensitive data. Front end portal access is controlled through permissions as described in 6(e). Only a select few individuals have access to the database, and the data within the database, and they must go through specific role-based training in order to gain access to such information. In addition, log files are created for all transactions, leaving an audit trail. The transactions are logged and the logs are regularly reviewed.

Modification of Data: The CABI Portal users do not have access to the “raw” source data and therefore, the data cannot be modified by the average user.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The CABI Portal does not collect information directly from individuals. An individual would need to contact the owner of the source system such as NIV, IVO, CEAC, and TDIS to request access to their information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐ Yes

☒ No

If yes, explain the procedures.

If no, explain why not.

The CABI Portal does not collect information directly from individuals. Our data is copied from the original source systems in a one-way pull from the source systems into our data warehouse. There is no way for a change to data in the CABI Portal data warehouse to be replicated back to the source system. In addition, if any data were changed in the CABI Portal data warehouse, it would most likely be overwritten by the original values from the source system during the next data pull. An individual can contact the owner of the source system such as NIV, IVO, TDIS, or CEAC to correct their information. Those corrections would then be replicated to the CABI Portal data warehouse during the next data pull.

(c) By what means are individuals notified of the procedures to correct their information?

CABI Portal does not collect PII from individuals and only pulls information, including PII, from the CCD database which resides outside the CABI Portal system boundary. Notification is the responsibility of the system that collects the information directly from the individual.

8. Security Controls

(a) How is the information in the system secured?

The Department of State also follows the full range of NIST 800-53 Revision 4 controls to secure the system. Specifically, this involves using a combination of technical, operational and managerial controls to achieve this. Technical controls utilized include using secure transmission methods. Operational examples include screening people carefully who will be working with the system, providing them with the required annual training on aspects of information security, and providing Commercial-Off-The-Shelf (COTS) products, like virus-control software, to provide standard protection of workstations used to access PII data. Management controls include annual review of the security controls of the system to ensure all aspects of information security continue to meet the NIST standards, which continually evolve to incorporate newer technologies and advanced guidance.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Internal access to the CABI Portal is limited to authorized State Department OpenNet users, including cleared contractors, who have a justified need for the information in order to perform official duties, and to auditors with the Office of Inspector General (OIG). To access the CABI Portal, users must first be granted the status of an authorized user of the State Department's unclassified network. Once that access has been granted, a user can then access the CABI Portal.

Access to information within the CABI Portal is role based and controlled by Business Objects security groups. Each report within the CABI Portal is assigned to a Business Objects security group. Each security group is also associated with either an Active Directory group or role in an external system. For a user to access a report, they must be part of the specific Active Directory (AD) group or have the external role associated with the Business Objects security group. The AD groups and external roles associated with the report are determined by the Business Units. Report access is granted by the administrator of the AD group that permits access to the report.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The level of access for the authorized user restricts the data that may be viewed. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited by both the Business Objects application and by the Oracle and HANA databases.

The Department of State follows the NIST Guidelines, and there are specific guidelines for audits and auditing as well as for physical and environmental protection.

The security posture will be considered in terms of operations and administration, audits and monitoring, and operational assurance. All system modifications are evaluated to prevent them from detracting or circumventing any established security or assurance controls.

(d) Explain the privacy training provided to authorized users of the system.

In accordance with Department of State computer security policies, all users are required to complete PS800 - Cyber Security Awareness Training annually as well as PA459 – Protecting Personally Identifiable Information. Upon accessing the CABI Portal, all users are presented with a Privacy Agreement which states:

> Information Protected under INA 222(f) and 9 FAM 40.4: This information "shall be considered confidential" per Section 222(f) of the Immigration and Nationality Act (INA) [8 U.S.C. Section 1202]. Access to and use of such information must be solely for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States under INA 222(f) and 9 FAM 40.4. Do not access this information in anything other than an official capacity, and do not share it without the permission of the Department of State.

In order to access the actual reports, the user must acknowledge that they have read the Privacy Agreement according to the following statement:

> I have read the Privacy Agreement and understand my responsibilities regarding the protection of passport and consular records.

The Department maintains a standard "Rules of Behavior" regarding the use of any computer system and the data it contains that require users to protect PII through appropriate safeguards to ensure security, privacy and integrity. The expectation is that all users of DoS's Passport Services Management Information System (MIS), the Visa Office's Pre-IVO Technology (pIVOt), the OCS Smart Traveler Enrollment Program Metrics (STEP Metrics), the BI CA RFID Tracking (BI CART) and other systems that use SAP Business Objects follow all the established guidelines and requirements. The responsibility to enforce this is held within the ISSO group at all levels.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

☒ Yes

☐ No

If yes, please explain.

The CABI Portal, as well as all Department of State internal web sites, are in the process of implementing SSL encryption (https://). The Bureau of Information Resource Management (IRM) has mandated that all sites implement SSL. We are currently working on a solution to implement SSL for the CABI Portal and plan to have it implemented by the end of FY18.

On the SAP HANA database, the Enterprise Reporting Team has implemented data encryption in the persistence layer. (Company name is SAP; HANA - High-performance ANalytic Appliance). This is referred to as data volume encryption in the HANA manuals and ensures that anyone who can access the data volumes on disk using operating system commands cannot see the actual data. The data volumes are encrypted using the AES-256-CBC algorithm. Pages are encrypted and decrypted using 256-bit page encryption keys. [Additional information can be found in the "SAP HANA Security Guide, SAP HANA Platform SPS12" Document Version: 1.1-2016-03-29.

(f) How were the security measures above influenced by the type of information collected?

The measures implemented are the result and consideration of the amount and type of PII that is collected. Due to the sensitivity of the information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing. The information collected contains PII of foreigners and U.S. Citizen / LPR. Although recourse for each group is different based on the Privacy Act of 1974 and INA 222(f), the PII is protected within the information system in the same manner.

9. Data Access

(a) Who has access to data in the system?

The CABI Portal may be accessed by authorized users within the Department of State. The reports and data that a user can see when accessing the CABI Portal depends on the permissions that have been granted to that user.

There are four types of user roles: Administrator, Alternate Administrator, Application Security managers and users.

Administrator and Alternate Administrator: System administrative staff maintains the system and user accounts, perform system backups, control access control lists, manage the operating system changes, etc. They have the same security responsibilities of users, but their responsibilities are expanded to recognize their privileged user status. Systems administrators restrict themselves from using their position to turn off/destroy audit trails, not to give unauthorized individuals privileged access, and not to modify the system to negate automated security mechanisms.

Application Security Managers: Security Managers administer and monitor the activities to protect the system. The Application Security Manager utilizes the Central Management Console to manage user access levels.

Users: Authorized individuals who acquire information from CABI to perform duties using generated reports dashboards, ad-hoc reporting tools, and analysis tools.

All access permissions are enforced by Business Objects groups according to the principle of least privilege and the concept of separation of duties. Business Objects groups are populated by linking them to an external authoritative source (AD group or external application role).

(b) How is access to data in the system determined?

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user’s particular job function and level of clearance.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒ Yes

☐ No

In addition to the NIST Guidelines being implemented, which is documented elsewhere in this report, the CABI Portal follows the CST System Development Lifecycle governance process.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No, all users will not have access to all data in the system. The CABI Portal has a very restrictive policy regarding accessing sensitive data. There is a process is in place whereby each Business Unit must define requirements and authorize users for all reports from CABI for which they are the data owners.

There are five types of user roles: (e.g.: Administrator, Alternate Administrator, Security, Power Users, and View Only). All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.)

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

In addition to access restrictions and annual security awareness training, numerous levels of auditing, identification and authentication, media protection, and system and information integrity are implemented to reduce the risk and misuse of privacy data by personnel.